Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

PROCEDIMIENTO INSTITUCIONAL PARA:

ATENDER INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Área responsable: Dirección de Tecnologías de la Información

Contenido

		Página
I.	Objetivo	2
II.	Ámbito de aplicación	2
III.	Interacción con módulos del SIIUAM	2
IV.	Insumo(s) y resultado(s)	2
V.	Áreas administrativas participantes en el análisis	2
VI.	Responsable de la revisión y actualización	2
VII.	Revisión y actualización	2
VIII.	Normatividad aplicable	3
IX.	Glosario	3
X.	Directrices del procedimiento	6
XI.	Normas de operación	6
XII.	Descripción del procedimiento	9
XIII.	Diagrama de flujo	11
XIV.	Lista de distribución de la versión electrónica del procedimiento con firmas	14
XV.	Control de cambios	14

Código: PI-DTI-07	Inicio de vigencia: 12 de enero de 2022	Núm. de actualización: 0		Núm. de páginas: 14
Elaboró: Mat. Carlos Luna Ortega Subdirector de Cómputo Académico	Revisión funcional: Mtro. Max Ulises de Mendizábal Carrillo Director de Tecnologías de la Información	Revisión técnica: Dr. Mauricio Sales Cruz Coordinador General de Información Institucional	Revisión jurídica: Mtro. Rodrigo Serrano Vásquez Abogado General	Autorizó: Dra. Norma Rondero López Secretaria General
Fecha de elaboración: 3 de noviembre de 2021	Fecha de revisión funcional: 8 de noviembre 2021	Fecha de revisión técnica: 11 de noviembre de 2021	Fecha de revisión jurídica: 15 de diciembre de 2021	Fecha de autorización: 12 de enero de 2022

I. Objetivo:

Establecer el procedimiento administrativo para identificar y atender los incidentes de seguridad de la información de los servicios proporcionados por la Dirección de Tecnologías de la Información.

II. Ámbito de aplicación:

El presente procedimiento es aplicable a las actividades derivadas de los servicios de Tecnologías de la Información.

III. Interacción con módulos del SIIUAM:

No aplica.

IV. Insumo(s) y resultado(s):

Insumo(s): Solicitud de servicio.

Resultado(s): Solicitud atendida.

V. Áreas administrativas participantes en el análisis:

En Rectoría General:

5.1 Secretaría General

5.2 Oficina del Abogado General

5.3 Dirección de Tecnologías de la Información

5.4 Dirección de Análisis y Seguimiento Institucional

5.5 Dirección de Comunicación Social

5.6 Dirección de Recursos Humanos

En unidades universitarias:

5.5 Áreas de Servicios de Cómputo

VI. Responsable de la revisión y actualización:

La Dirección de Tecnologías de la Información será responsable de revisar y actualizar este procedimiento.

VII. Revisión y actualización:

El presente procedimiento será revisado y actualizado si se modifica la normatividad aplicable, el proceso administrativo o de mejora continua; por inserción tecnológica o por revisión bianual.

VIII. Normatividad aplicable:

Legislación nacional:

8.1 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

8.2 Ley General de Archivos.

Legislación universitaria:

8.3 Ley Orgánica.

8.4 Reglamento Orgánico.

8.5 Reglamento para la Transparencia de la Información Universitaria.

IX. Glosario:

9.1 Persona administradora de Elemento de Configuración: trabajadora o trabajador especialista de la Dirección de Tecnologías de la Información responsable de modificar la configuración y mantener operando un Elemento de Configuración.

9.2 Persona administradora de Incidentes de Seguridad de la Información: trabajadora o trabajador de la Dirección de Tecnologías de la Información responsable de calificar el incidente, la toma de decisiones y la gestión del incidente de seguridad de la información, considerando los criterios generales establecidos para la seguridad de la información.

9.3 Persona administradora de incidentes: trabajadora o trabajador de la Dirección de Tecnologías de la Información que participa en la coordinación, supervisión y seguimiento de las actividades para la atención de los incidentes.

9.4 Persona administradora de Mesa de servicios: trabajadora o trabajador de la Dirección de Tecnologías de la Información que tiene la responsabilidad de gestionar las actividades de la Mesa de servicios.

9.5 Área de soporte: grupo de trabajo de la Dirección de Tecnologías de la Información que cuenta con los conocimientos y habilidades para resolver una solicitud de servicio, clasificada en una categoría del catálogo de la Mesa de servicios.

9.6 Cadena de custodia: registro de la recopilación, posesión y resguardo de las evidencias encontradas durante la atención de un incidente de seguridad de la información.

9.7 Componente de Infraestructura: elemento de hardware o software que sustenta un servicio de la Universidad.

9.8 Elementos de configuración: componente que forma parte de un servicio de tecnologías de la información y comunicaciones, los cuales pueden ser hardware, software, licencias, contratos y otros similares.

9.9 Entidad externa: instancia o persona que no forma parte de la comunidad universitaria que detecta y notifica el incidente de seguridad de la información.

9.10 Equipo de Respuesta a Incidentes de Seguridad de la Información: grupo de trabajo de la Universidad (órganos personales e instancias de apoyo) responsable de toma de decisiones y personas especialistas que atenderán un incidente de seguridad de la información que afecte de manera significativa el capital humano, los bienes, los recursos financieros y la imagen de la Universidad. Estará integrado de manera permanente por representantes de la Secretaría General, la Oficina del Abogado General y la Dirección de Tecnologías de la Información, así como de las personas titulares de áreas de Recursos Humanos, Comunicación Social, de acuerdo con su competencia.

9.11 Fallo en las configuraciones: condición no esperada que afecta el funcionamiento de las aplicaciones o la infraestructura.

9.12 Grupo de Análisis de Incidentes de Seguridad de la Información: conjunto de personas que integran un equipo interdisciplinario conformado por especialistas en tecnologías de la información y comunicaciones de la Universidad, áreas usuarias, proveedores de servicios o entidades externas que proponen alternativas para la resolución del incidente de seguridad de la información.

9.13 Impacto: grado de desviación sobre la operativa normal de un servicio, que se mide en términos del número de las áreas usuarias o de procesos de los servicios afectados.

9.14 Incidente de Seguridad de la Información: evento que compromete la confidencialidad, la integridad o la disponibilidad mediante un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento en la operación normal de las redes, sistemas o recursos informáticos; violación a la normatividad interna de la Universidad.

9.15 Incidente: interrupción o disminución no planeada de un servicio.

9.16 Incidentes no intencionados: eventos que afectan a los activos de información y son originados por errores humanos o situaciones circunstanciales.

9.17 Información: es un conjunto de datos que, vistos como un todo, adquieren significado y valor. Se encuentra en formato impreso, digital y conceptual.

9.18 Mesa de servicios: unidad funcional de la Dirección de Tecnologías de la Información responsable de gestionar y dar cumplimiento a las solicitudes de servicios, cambios y atención de incidentes.

9.19 Pérdida de información: daño parcial o total de información en proceso, transportación o almacenamiento.

9.20 Prioridad: dígito entre uno y cinco, que representa la urgencia con la que se atenderá el incidente, debido al impacto en los servicios o a la afectación en el usuario, los bienes, los recursos financieros y la imagen de la Universidad. El uno representa la más alta urgencia y el cinco la más baja.

9.21 Protección de evidencia: recopilación y resguardo de material probatorio que permita identificar las causas, formas y consecuencias de un incidente de seguridad de la información.

9.22 Seguridad de la información: es la protección de la confidencialidad, integridad y disponibilidad de la información en general para atender las necesidades de las personas que están autorizadas a usarla de acuerdo con criterios establecidos (permisos, clasificación, lineamientos, etc.).

9.23 Seguridad informática: acciones necesarias para establecer y mantener la protección del entorno virtual conformado por el Internet, las personas, las organizaciones, las redes y los dispositivos. Incluye la aplicación de tecnologías, procesos y controles para proteger sistemas, redes, programas, dispositivos e información de ataques cibernéticos.

9.24 Situación de crisis: incidente que por la gravedad en el impacto en los servicios y la urgencia para resolverlo puede generar una situación que compromete a la operación de la Universidad.

9.25 Solución definitiva: acciones que permiten no tener recurrencia del incidente.

9.26 Solución temporal: acciones para evitar o mitigar un incidente mientras se encuentra la solución definitiva del mismo.

9.27 Tercero: proveedor de servicios que no forma parte de la Universidad, que participa en la solución del incidente de seguridad de la información.

9.28 Titular de Área de Soporte Asignado: trabajadora o trabajador de la Dirección de Tecnologías de la Información, con la responsabilidad de gestionar el cumplimiento de las solicitudes asignadas a su categoría.

9.29 Titular de Área de Soporte: trabajadora o trabajador de la Dirección de Tecnologías de la Información responsable de asignar una solicitud de servicio a un Trabajador de Área de Soporte Asignado.

9.30 Urgencia: situación que requiere de toma de decisiones inmediata para resolver el incidente.

9.31 Usuaria(o) de Mesa de servicios: trabajadora o trabajador de la Universidad que utiliza los servicios de tecnologías de información y comunicaciones.

9.32 Usuaria(o) externa(o): aspirantes, proveedores, entre otros interesados que utilizan los servicios de tecnologías de la información y comunicaciones.

9.33 Usuaria(o) UAM: cualquier miembro del alumnado, del personal administrativo o académico adscrito a la Universidad.

Siglas:

AISI: Administrador de Incidentes de Seguridad de la Información.

DTI: Dirección de Tecnologías de la Información.

ERISI: Equipo de Respuesta a Incidentes de Seguridad de la Información.

GAINSI: Grupo de Análisis de Incidentes de Seguridad de la Información.

SIIUAM: Sistema Integral de Información de la Universidad Autónoma Metropolitana.

TAS: Titular del Área de Soporte.

TASA: Trabajador del Área de Soporte Asignado.

UAM: Universidad Autónoma Metropolitana.

X. Directrices del procedimiento:

10.1 Contribuir a la eficiente atención en los servicios de cómputo bajo los principios de seguridad, integridad de la información y transparencia.

10.2 Establecer el nivel de responsabilidad de las áreas que intervienen en el procedimiento.

10.3 Reducir el daño hacia el usuario UAM, los bienes, los recursos financieros y la imagen de la Universidad, derivado de un incidente de seguridad de la información.

XI. Normas de operación:

Acerca de la recepción de solicitudes:

11.1 Las áreas usuarias de la Mesa de servicios que cuenten con la aplicación en web podrán registrar la solicitud de servicio por ese medio.

11.2 Las áreas usuarias de la Mesa de servicios que no tengan acceso a la aplicación en web podrán realizar la petición del servicio por medio de:

- Cuentas de correo electrónico publicadas en la página web de la Mesa de servicios.
- Llamada telefónica a las extensiones publicadas en la página web de la Mesa de servicios.

11.3 Para el registro de las solicitudes, las áreas usuarias deberán apegarse al catálogo de servicios establecido por la DTI, disponible en la página web de la Mesa de servicios.

11.4 Para las áreas usuarias de las unidades universitarias, la solicitud del servicio aplicará para las categorías que tengan derecho a la Mesa de servicios.

11.5 La trabajadora o el trabajador que detecte o tenga conocimiento de un incidente deberá informar de inmediato a la persona responsable del servicio correspondiente o, en su caso, a la jefa o al jefe inmediato.

11.6 La persona titular del Área de Soporte será responsable de identificar si la solicitud recibida es un incidente de seguridad de la información y, en caso de serlo, deberá notificar al AISI.

11.7 El AISI será responsable de verificar si la solicitud recibida es un incidente de seguridad de la información y, en caso de serlo, deberá clasificarlo en el sistema.

Acerca de la atención de incidentes de seguridad de la información:

11.8 Las *Solicitudes de atención de incidentes de seguridad de la información* se atenderán en función de la urgencia y el impacto adverso hacia las operaciones y los activos de la Universidad, estableciendo la prioridad según la tabla siguiente.

Tabla de prioridad		Impacto		
		Alto	Medio	Bajo
Urgencia	Alta	1	2	3
	Media	2	3	4
	Baja	3	4	5

* La definición de los criterios se puede consultar en la Mesa de servicios.

Descripción	Prioridad
Crítico	1
Alto	2
Medio	3
Bajo	4
Menor	5

11.9 Las trabajadoras o trabajadores de la DTI que intervengan en la solución de un incidente deberán tomar en cuenta el calendario de procesos críticos de la Universidad, el cual será proporcionado por las personas titulares de las Subdirecciones de la DTI.

11.10 En caso de ser necesario, el AISI consultará con el TASA del área específica donde se presentó el incidente las condiciones en las que se suscitó, para resolverlo de manera conjunta, previa consulta con el TAS.

11.11 En caso de que el incidente requiera el soporte de alguna dependencia universitaria en unidades, el TASA deberá dirigirse a la Coordinación de Servicios de Cómputo que corresponda y, si fuera necesario, a la instancia que refiera dentro de dicha Unidad.

11.12 El AISI será responsable de convocar al GAINSI cuando así se requiera.

11.13 Será responsabilidad del AISI, en colaboración con el GAINSI, restablecer a la brevedad posible el servicio, ya sea mediante una solución temporal, definitiva o, en su caso, aplicar soluciones alternas.

11.14 Las trabajadoras o trabajadores de la DTI implementarán a la brevedad posible, la contención en función del tipo de incidente, limitando el alcance y la afectación producida por el incidente.

11.15 Para la implementación de la solución tecnológica el AISI podrá solicitar los registros, bitácoras y respaldos de los elementos de configuración a sus administradores.

Acerca del cierre de incidentes de seguridad de la información:

11.16 La información que deberá registrarse al cierre del incidente en la Mesa de servicios será integrada conforme al formato de *Registro de Incidentes de Seguridad de la Información*.

Acerca de la documentación de incidentes de seguridad de la información:

11.17 El AISI, con la información obtenida de las trabajadoras o los trabajadores de la DTI, proveedores, fabricantes o dependencias universitarias que intervinieron en la solución del incidente, realizará el *Registro de Incidentes de Seguridad de la Información*, a más tardar cinco días hábiles después de atenderlo.

11.18 La persona administradora de la Mesa de servicios deberá entregar de manera mensual, semestral y anual los reportes solicitados por el AISI.

11.19 El AISI será el responsable de coordinar la recopilación y preservación de la evidencia (cadena de custodia).

Acerca de la confidencialidad del resultado del reporte de incidentes de seguridad de la información:

11.20 El GAINSI será el responsable de asignar el nivel de confidencialidad de los reportes de incidentes de seguridad de la información que atendió.

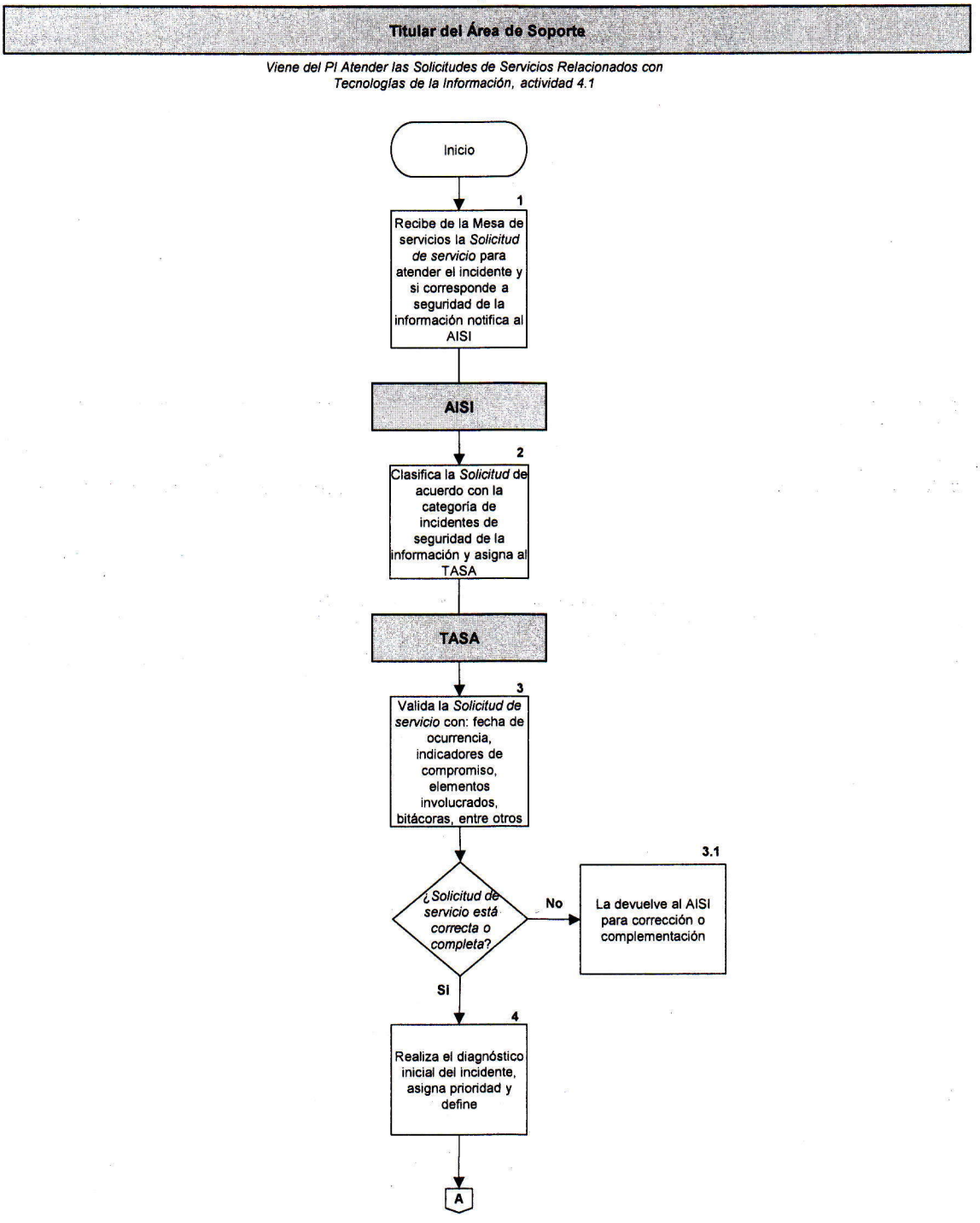
XII. Descripción del procedimiento:

Responsable	Núm.	Actividad
		Viene del Procedimiento Institucional para Atender las Solicitudes de Servicios Relacionados con Tecnologías de la Información, actividad 4.1
Titular del área de soporte:	1	Recibe de la Mesa de servicios la *Solicitud de servicio* para atender el incidente y, una vez que identifica que corresponde a seguridad de la información, notifica al AISI.
AISI:	2	Clasifica la *Solicitud* de acuerdo con la categoría de incidentes de seguridad de la información en la Mesa de servicios y asigna al TASA.
TASA:	3	Valida la *Solicitud de servicio* con: fecha de ocurrencia, indicadores de compromiso, elementos involucrados, bitácoras y capturas de pantalla, entre otros. 3.1 Si la *Solicitud de servicio* es incorrecta o está incompleta devuelve a la AISI para su corrección o complementación.
	4	Si la *Solicitud de servicio* es correcta y está completa, realiza el diagnóstico inicial del incidente, le asigna prioridad y define: a. Puede resolverlo. b. Requiere soporte del proveedor o fabricante o alguna dependencia universitaria. c. No puede resolverlo.
	5A	En caso de poder resolverlo evalúa las acciones a seguir, implementa la solución tecnológica y notifica al AISI. ***(Continúa con la actividad 10)***
	5B	Si requiere el soporte del proveedor, fabricante o alguna dependencia universitaria, según corresponda, lo solicita y notifica al AISI.
	5B.1	Recibe el soporte del proveedor, fabricante o dependencia universitaria e implementa las acciones que dan solución tecnológica al incidente y notifica al AISI. ***(Continúa con la actividad 10)***
	5C	Si no puede resolverlo, notifica al AISI y le solicita que convoque al GAINSI.
AISI:	5C.1	Recibe la notificación, convoca al GAINSI y le envía el diagnóstico inicial.
GAINSI:	5C.2	Realiza el diagnóstico del incidente de seguridad de la información, le asigna prioridad, determina el impacto, comunica implicaciones a especialistas de la DTI, áreas de apoyo y Subdirecciones para definir si: a. Puede resolverlo. b. La solución tecnológica requiere aprobación del ERISI. 5C.2.A Evalúa las acciones a seguir e indica al AISI las actividades para articular la implementación de la solución tecnológica. ***(Continúa con la actividad 10)***

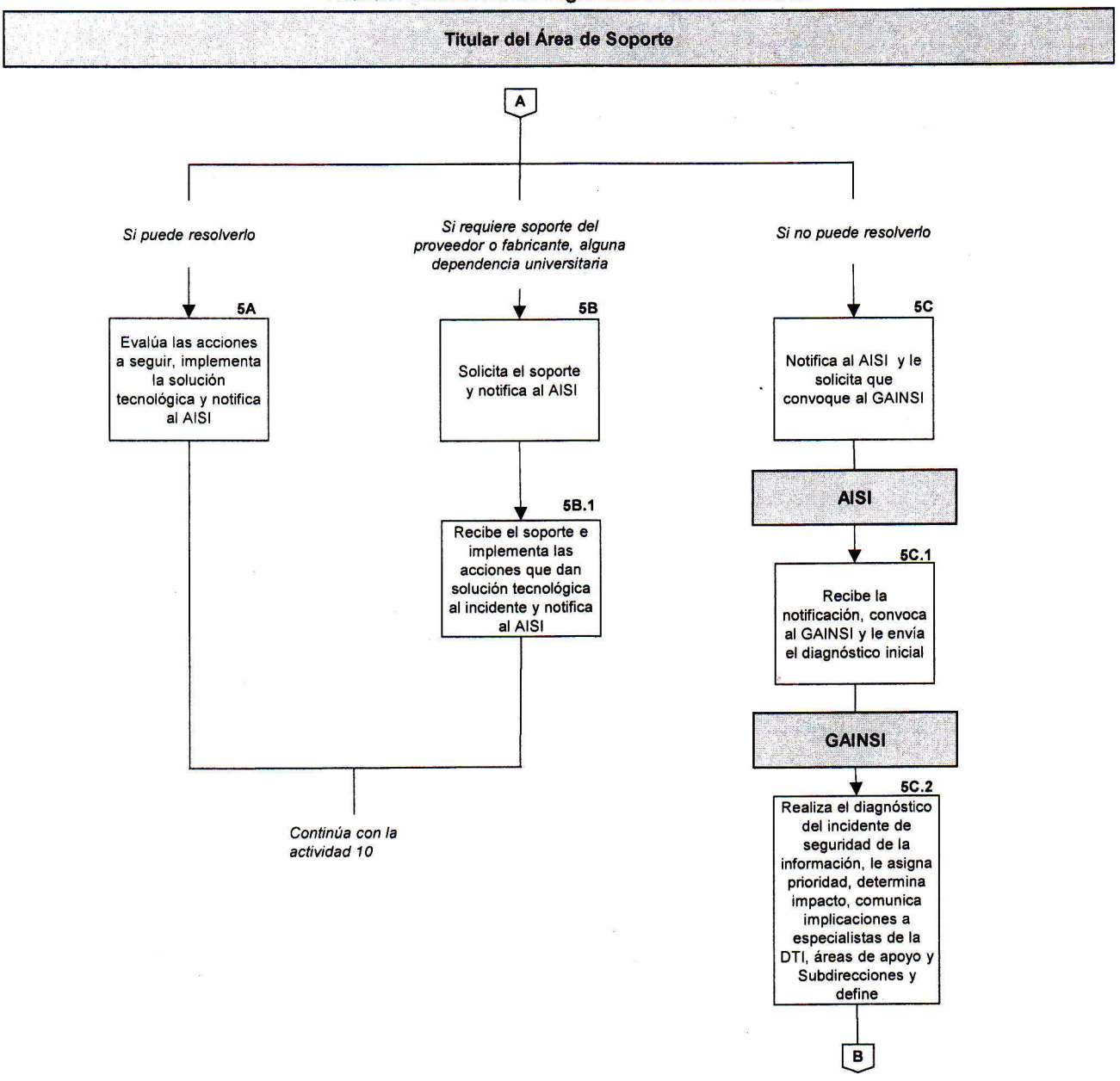
Responsable	Núm.	Actividad
GAINSI:		5C.2.B Convoca al ERISI para solicitar la aprobación de la solución tecnológica del incidente.
ERISI:	6	Evalúa las acciones y notifica por escrito el resultado al GAINSI.
GAINSI:	7	Recibe la notificación y revisa.
		7.1 Si la notificación sobre la solución tecnológica no procede, evalúa las soluciones alternas para mitigar el daño y en su caso las aplica. ***(Continúa con la actividad 10)***
	8	Si la notificación sobre la solución tecnológica procede indica al AISI las acciones realizar.
AISI:	9	Articula las actividades para la implementación de la solución tecnológica.
	10	Una vez que se aplicó la solución tecnológica o, en su caso, la solución alterna, llena el registro de incidente de seguridad de la información, lo entrega a su jefe inmediato y cierra la *Solicitud* en la Mesa de servicios.
		Fin del procedimiento

XIII. Diagrama de flujo:

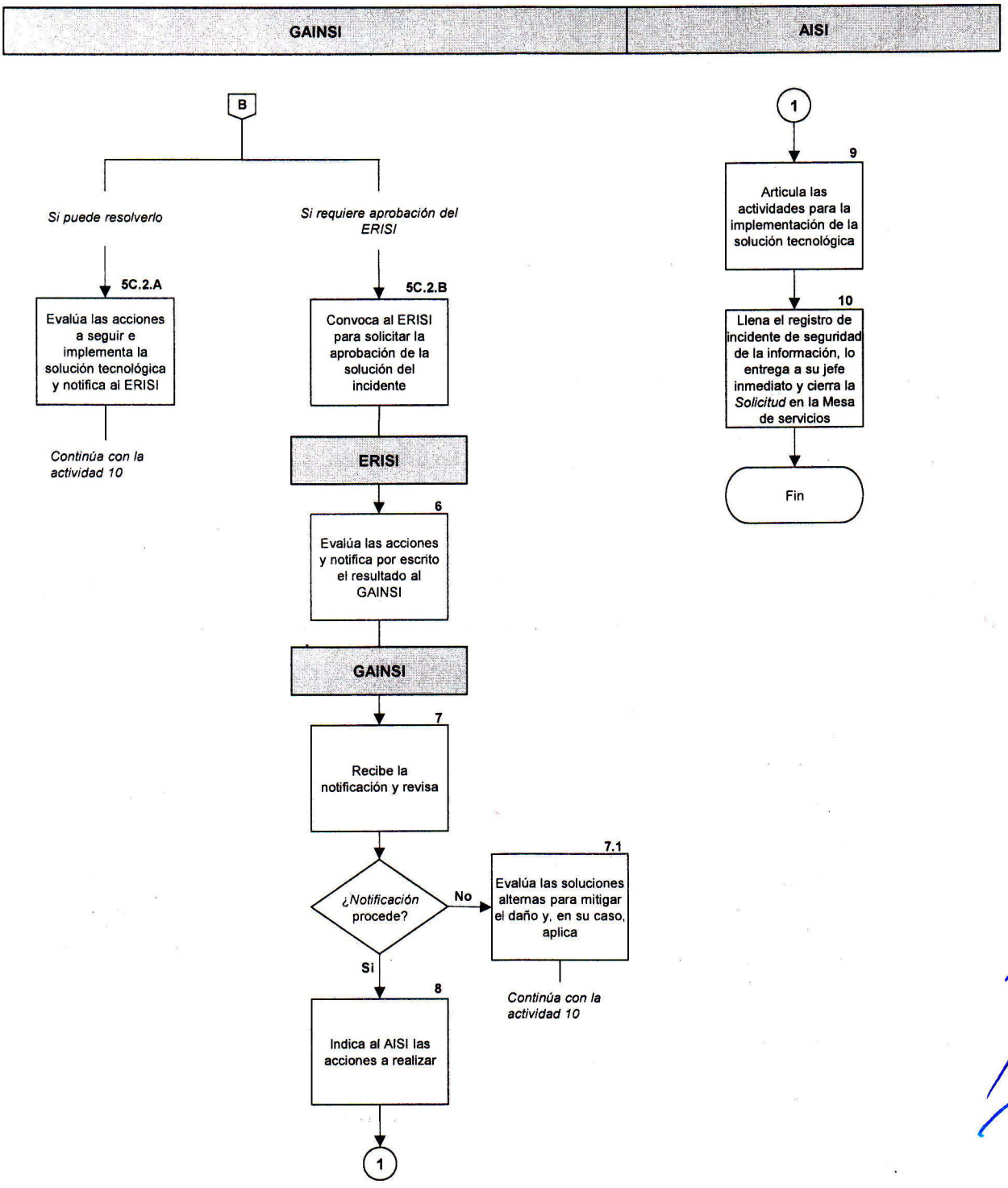
Atender incidentes de seguridad de la información



Atender incidentes de seguridad de la información



Atender incidentes de seguridad de la información



XIV. Lista de distribución de la versión electrónica del procedimiento con firmas:

En Rectoría General:

14.1 Secretaría General.

14.2 Oficina del Abogado General.

14.3 Contraloría.

14.4 Tesorería General.

14.5 Coordinación General de Administración y Relaciones Laborales.

14.6 Coordinación General de Difusión.

14.7 Coordinación General para el Fortalecimiento Académico y Vinculación.

14.8 Coordinación General de Información Institucional.

En unidades universitarias:

14.9 Secretaría de Unidad.

14.10 Coordinación de Servicios de Cómputo.

14.11 Coordinación de Servicios de Información y Comunicaciones.

La difusión en medios electrónicos se realizará en la sección de procedimientos institucionales en la página web de la Universidad.

XV. Control de cambios:

Revisión Núm.	Fecha	Hoja Núm.	Motivo o Causa
No aplica			